

Решение Dell PowerProtect Cyber Recovery

Восстановление вашего бизнеса после комплексных атак вирусов-вымогателей или кибератак

Сергей Шатохин
Старший системный инженер
Dell Technologies Central Asia

Не Если....

НО Когда

События, которые когда-то считались экстремальными и необычными, теперь стали обыденностью

DELLTechnologies

Широкий спектр комплексных киберугроз

Мотивации, Техники и Цели



Криминал



Шпионаж



Терроризм



Инсайдер



Хактивизм



Война

Cyber Resilience

это стратегия.

Комплексная стратегия высокого уровня, включающая стандарты кибербезопасности, рекомендации, людей, бизнес-процессы и технологические решения.

Пример: [NIST Cybersecurity Framework](https://en.wikipedia.org/wiki/Cyber_resilience)



Cyber Recovery это решение.



Решение по защите данных, которое изолирует критически важные для бизнеса данные от атак.

Критически важные данные хранятся в неизменном виде в защищенном хранилище, что позволяет восстанавливать данные с гарантированной доступностью, целостностью и конфиденциальностью.

Disaster Recovery это не Cyber Recovery

Disaster Recovery / Business Continuity – этого не достаточно для ответа современным киберугрозам

Категория	DISASTER RECOVERY	CYBER RECOVERY
Время восстановления	Почти мгновенно	Надежно и быстро
Точка восстановления	В идеале непрерывно	В среднем 1 день
Природа катастрофы	Наводнение, отключение электроэнергии, погода	Кибератака, направленная
Влияние катастрофы	Региональное, распространение сдерживается	Глобальное; распространяется быстро
Топология	Связная, множество целей	Изолированная, дополнение к DR
Объем данных	Полный, все данные	Выборочный, включает базовые сервисы
Восстановление	Стандартный DR (откат)	Итерационное, выборочное восстановление; часть CR

Требования Cyber Recovery

Современные угрозы требуют инновационных решений



Неизменность данных с PowerProtect Data Domain

Основа защиты данных для обеспечения
устойчивости

Серия PowerProtect Data Domain

Основа для защиты данных



Avamar – Networker – Data Manager
Data Protection Advisor – DD Series

Retention Lock Compliance (Immutability)

SEC 17a-4f Compliance

Role Based Access

End to End Encryption

Dual Role Authorization

Multi-Factor Authentication

Secure System Clock

NTP Clock Tamper Controls

Key Management

Custom System DDOS

DD File System Hardened

DDBoost

Integrated Lights Out Mgt Hardening (iDRAC)

Data Invulnerability Architect (DIA)

Secure AD/LDAP Authentication

Secure Remote support

Anomaly Reporting with DPA



DELLTechnologies



Изоляция с PowerProtect Cyber Recovery

Абсолютное решение для восстановления
после кибератак



Dell Technologies

Путь успеха PowerProtect Cyber Recovery

2015	Первое “Изолированное” решение по восстановлению с кастомизированным внедрением
2018	Анонс решения PowerProtect Cyber Recovery
2019	Первый технологический вендор в партнерской программе Sheltered Harbor Alliance
2020	Первое одобренное Sheltered Harbor решение – PowerProtect Cyber Recovery
2021	Появление Cyber Recovery с Multi-Cloud Data Services для Dell PowerProtect
2021	Появление PowerProtect Cyber Recovery для AWS
2021	Поддержка PowerProtect Cyber Recovery для DLm
2022	Появление PowerProtect Cyber Recovery для Azure и Google Cloud
2022	Управляемые сервисы as-a-Service APEX Cyber Recovery
2023	Услуги по ускорению успеха продукта (PSX) для PowerProtect Cyber Recovery

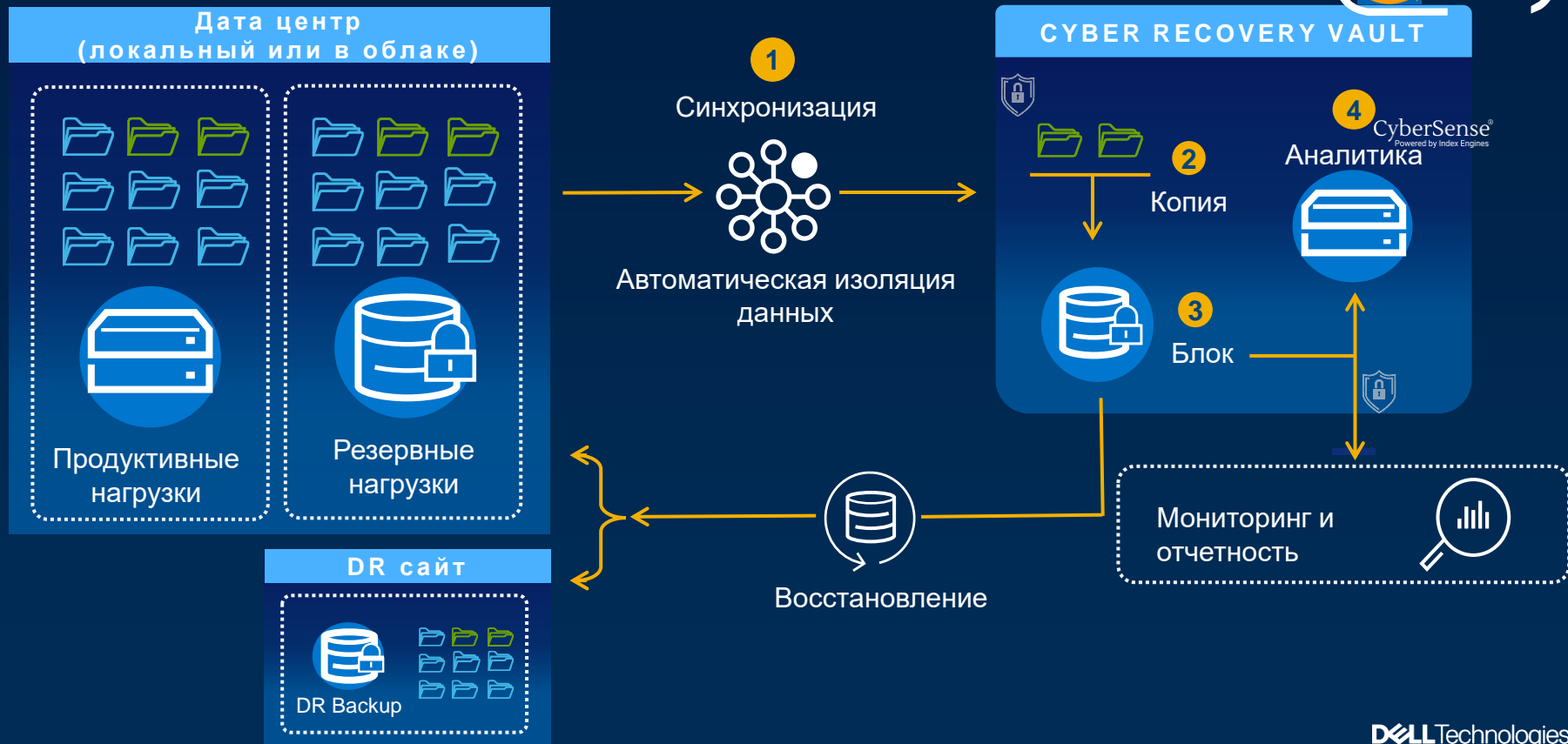
2300+

Заказчиков Cyber Recovery¹

¹ Based on Dell Technologies internal analysis, July 2024

Dell PowerProtect Cyber Recovery

Обеспечение восстановления критически важных данных в случае киберугроз



Важность изолирования

Улучшение неизменяемости путем запрета доступа



Более умное восстановление с CyberSense

Упрощенная панель инструментов для аналитики и отчетности



Вид панели инструментов

- Простое представление о работоспособности аналитической среды
- Обнаружение повреждений цикла резервного копирования
- Расследование атаки - Кто, Что, Где и Когда
- Быстрая идентификация последней «чистой» копии для восстановления

The screenshot displays the CyberSense dashboard interface. At the top, there are navigation tabs: Home, Alerts (41), Hosts, Backups, Policies, and Settings. A 'Welcome admin' message is visible in the top right corner. The main content area is divided into several sections:

- Welcome to CyberSense:** A header section with a 'Download' button and the date range 'May 07, 2024 - June 07, 2024'.
- License Expiration:** A card showing the expiration date '2/21/2025'.
- Hosts Analyzed:** A card showing the count '7'.
- Files Analyzed by Backup Type:** A bar chart showing the number of files analyzed for different backup types (windows, unix, linux, generic) from 5/08/24 to 5/16/24.
- Policies:** A card showing the count '9'.
- Files Analyzed:** A card showing the count '12,576,477'.

Below these cards, there is a brief description of CyberSense's capabilities: 'CyberSense conducts comprehensive full content scans to verify the integrity of both files and databases, guaranteeing the reliability of data ransomware attack. CyberSense is architected to detect malicious corruption by known variants of ransomware, encompassing a wide range of tactics such as full extensions. Additionally, it scrutinizes databases for comprehensive changes, including full file alterations, as well as page and table corruption.'

The **Alerts** section is highlighted with a green box. It shows a table of alerts with columns for Severity, Type, Details, Backup Time, Policy, Host, and Backupset. A critical alert is highlighted:

SEVERITY	TYPE	DETAILS	BACKUP TIME	POLICY	HOST	BACKUPSET
Critical	Incremental	Infection was found in...	3/11/2024 9:04:55 pm	NFS_manual	192.168.192.198	192.168.192.198.03.19.2024 at 12...
Critical	Full	Infection was found in...	9/3/2024 11:37:46 AM	ql_test_2024-03-19-NFS_dbss96-A	cybeross-horik	cybeross-horik_1536695048

The critical alert details are expanded to show: '2/2/2024 10:32:39 am: Database Corruption'. The description states: 'This alert does not suspect files, numbers of hosts infected, or graph information. Policy Name: jobname11681a2eead20c7966cc389ca950c7081010 Engine ID: C454381-CE-0549 Hosts: 91608a2e'. There are buttons for 'Alert Configuration', 'Show Files', and 'Clear'.

Below the alerts table, there is a section for 'Files for 2/2/2024 10:32:39 am: Database Corruption'. It shows a summary: '2 Suspect Files | 1 Hosts | Added Files | Deleted Files | Modified Files'. A table below shows the details of the suspect files, with columns for Host, Extension, and Modified Times.

Спасибо!

